Computers, Materials & Continua
DOI:10.32604/cmc.2021.012877
Article

Tech Science Press

Few-Shot Learning for Discovering Anomalous Behaviors in Edge Networks

Merna Gamal[1], Hala M. Abbas[2], Nour Moustafa[3,*], Elena Sitnikova[3] and Rowayda A. Sadek[1]

[1]Department of Information Technology, Helwan University, Cairo, Egypt
[2]Department of Computer Science, Helwan University, Cairo, Egypt
[3]School of Engineering and Information Technology, University of New South Wales at ADFA, Canberra, Australia
[*]Corresponding Author: Nour Moustafa. Email: nour.moustafa@unsw.edu.au
Received: 30 August 2020; Accepted: 16 April 2021

Abstract: Intrusion Detection Systems (IDSs) have a great interest these days to discover complex attack events and protect the critical infrastructures of the Internet of Things (IoT) networks. Existing IDSs based on shallow and deep network architectures demand high computational resources and high volumes of data to establish an adaptive detection engine that discovers new families of attacks from the edge of IoT networks. However, attackers exploit network gateways at the edge using new attacking scenarios (i.e., zero-day attacks), such as ransomware and Distributed Denial of Service (DDoS) attacks. This paper proposes new IDS based on Few-Shot Deep Learning, named CNN-IDS, which can automatically identify zero-day attacks from the edge of a network and protect its IoT systems. The proposed system comprises two-methodological stages: 1) a filtered Information Gain method is to select the most useful features from network data, and 2) one-dimensional Convolutional Neural Network (CNN) algorithm is to recognize new attack types from a network's edge. The proposed model is trained and validated using two datasets of the UNSW-NB15 and Bot-IoT. The experimental results showed that it enhances about a 3% detection rate and around a 3%–4% false-positive rate with the UNSW-NB15 dataset and about an 8% detection rate using the BoT-IoT dataset.

Keywords: Convolution neural network; information gain; few-shot learning; IoT; edge computing

1 Introduction

The Internet of Things (IoT) plays a significant role in constructing smart systems, including smart homes, smart cities, and healthcare, to offer automated services to users and organizations [1]. The IoT can be defined as a communication model in which any device acts as an object that exchanges data through the Internet and senses the environment [2]. It consists of many IoT peripherals such as sensors and actuators that connect with the Internet. With the prevalence of IoT systems, network architectures have been redesigned to include three tiers of edge/physical, fog, and cloud [3]. The edge tier includes all computer devices, IoT devices, and network appliances [4]. This layer is linked with the fog tier, which is the interface that includes

virtualization platforms and gateways. Both layers are interconnected with the cloud tier that offers software, platforms, and infrastructure services to end-users [3,5].

The technology of IoT provides different functions that can interconnect devices and applications, along with computing resources, to handle the data captured [6]. The security of IoT systems is still the main challenge in the cybersecurity domain, due to the heterogeneity of IoT devices and the large number of IoT services linked to the network [3]. Manufacturers often do not plug security services to their IoT products, exceptionally light devices-enabled IP addresses, due to their non-standard and licensed firmware [4]. This leads to various vulnerabilities, either in the firmware or network level, in which attackers attempt to breach IoT systems and their networks. There are three security challenges in IoT networks [7]. Firstly, physical impendence in the edge layers results from weaknesses of hardware protection. Secondly, this is followed by a confidentiality challenge that discloses sensitive information of IoT services passed to the fog and cloud layers. Man-In-The-Middle (MITM) and reconnaissance attacks are common hacking techniques that violate the confidentiality of IoT networks. The cyber threat of confidentiality is often risky between gateways and IoT devices at the edge. Thirdly, the integrity challenge that alters or manipulates original data of IoT systems that breach privacy. This often happens using spoofing, poisoning, evasion, and inference attacks that steal and/or illegally modify the telemetry data of IoT systems and their networks [8,9].

The security and privacy of IoT networks are essential, which need to safeguard the IoT components that depend on object identification technologies. Every IoT object has its own identity that loads all its information, such as location and personal information. To monitor IoT systems' services at the edge of a network, defensive mechanisms, such as Intrusion Detection Systems (IDSs), should be effectively deployed and configured. The discovery of cyber-attacks at the edge layer would address the security issue in IoT networks. IDSs have been widely proposed to monitor and recognize cyber-attacks in network systems. However, existing network IDSs still suffer from the challenge of detecting new attack families (i.e., zero-day attack), especially with the extensive amount of network traffic collected from heterogeneous IoT systems across network connectivity [7,10]. Some IDSs have been explored in the literature to utilize shallow and deep learning techniques to discover cyber threats. A shallow network is declared as an artificial neural network that consists of one/two hidden layers. Deep learning (DL) is considered an improvement of shallow learning, but the difference is that deep learning has many hidden layers with different architectures [11]. Researchers have broadly used DL techniques in many fields, such as image processing, biomedical, and security. The shallow networks have achieved reasonable outputs in detection accuracy and low false alarm rates, for handling small-scale data. However, large-scale data demand a deep adaptive architecture that can learn hidden patterns and extract characteristic data features of anomalous behaviors in real-time, as we suggest in this study.

We propose using Few-Shot Learning (FSL) architecture [12] to address this challenge, which can deal only with a limited number of instances in time-series analysis of network traffic. In more detail, this paper proposes a new IDS using a few shot deep learning models that can discover cyber-attacks from the edge of a network. The proposed system includes two methodological phases: feature selection and decision engine. In feature selection, a filtered information gain method is employed to select the most useful features from network data. This phase improves the processing times and enhances the performance of the decision engine. Few-Shot Deep Learning techniques are utilized in the decision engine using an adaptable Convolutional Neural Network (CNN) architecture [13]. CNN is used to recognize new attack types from the network's

edge. The proposed work is trained using two-benchmark datasets of the UNSW-NB15 [14] and Bot-IoT [15].

The rest of the paper is structured as follows. Section 2 presents the background and related work of IoT and IDS. Section 3 explains the proposed approach for the intrusion detection system. Section 4 describes the empirical results and discussions. Finally, Section 5 introduces the conclusion of the paper.

2 Background and Related Work

This section explains the background and previous studies related to IDS and IoT networks.

2.1 Intrusion Detection System

An Intrusion Detection System (IDS) is a security solution, either hardware or software, which monitors network traffic and/or audit traces of client systems to identify cyber threats from computer and network systems [1]. Some IDSs react to intrusions in a real-time manner, while others do not work in real-time due to performing depth analysis for forensic purposes [16]. An IDS is essential software that monitors the traffic of the network that recognizes malicious events [17]. It mainly includes three stages: 1) a data preprocessing method is to filter and clean data; 2) an intrusion detection method is to train and test legitimate and suspicious observations; and 3) a decision-making method is to alert malicious events [5].

There are two popular forms of IDSs-based deployment: Host-based IDS (HIDS) and Network-based IDS (NIDS) [18]. One the one hand, a HIDS monitors system activities of hosts, for example, system configuration, application activity, system logs, application processes, and file access [19]. On the other hand, a NIDS monitors network activity and analyzes the collected information to identify suspicious events from network traffic [20]. The NIDS consumes low computational processing less than the HIDS and has a quicker response because it does not require maintaining for the sensor programming at the host level [1]. There are three detection methods in IDSs: 1) anomaly-based detection, 2) misuse-based detection, and 3) a hybrid of both. An anomaly detection method designs a standard profile and discovers outliers as anomalies [21]. A misuse-based detection method depends on well-known signatures and matches them against a blacklist of suspicious events. A misuse-based IDS cannot discover new attack types while An anomaly-based IDS can detect them, along with a false alarm rate if small variations of normal and abnormal patterns have been identified [22,23].

IDSs have been designed based on machine and deep learning algorithms to recognize cyber threats [1,5]. Deep learning algorithms have proven their capability in different applications, such as computer vision and malware detection [5]. Deep learning can be categorized on its architecture into generative and discriminative. The classes of generative architecture are Recurrent Neural Network (RNN), Deep Auto Encoder, Deep Boltzmann Machine (DBM), and Deep Belief Networks (DBN) [1]. Auto-encoder consists of two symmetrical components, which are an encoder and a decoder. The encoder works to extract the features from the raw data. The decoder reshapes the data from the features that extract using the encoder. DBM consists of arbitrary units for the whole network for getting or producing binary results. DBN has multiple layers that have a connection between them, not between units. Discriminative architecture has two types, which are recurrent neural network and convolutional neural network. RNN is used in sequential data, and in most cases, it is used for natural language processing [16]. This work focuses on CNN as it includes multiple layers that can classify small variations of data features of various class labels, such as legitimate and normal behaviors.

2.2 Internet of Things (IoT)

The Internet of Things (IoT) offers connecting devices and applications to the Internet to sense and monitor systems [4,16]. IoT is defined as the seamless connection of the information network and physical objects, named 'smart objects,' with these objects being active users in business processes, being accessed through network services, along with considering security and privacy in mind [24]. At the end of the 20th century, the Internet started to spread through web services. It was imaginable that objects like a pen or book that would automatically work itself and write directly. The development of IoT spreads worldwide through mobile devices, laptops, and workstations [3]. The creation of new IoT products would minimize the computer and new approaches linked with wireless networks [25]. Nowadays, IoT sensors connect to the Internet, such as devices that carry IP cameras. The IoT devices usually are not expensive and easy to deploy in IoT networks, such as the deployment of temperature and light bulb sensors [26].

Research studies have emphasized that security in the IoT concentrates on attack detection, authorization, authentication, and access control [26,27]. Many aspects affect the change of the traffic pattern while recognizing abnormal behaviors from IoT networks. It is vital to consider various aspects while developing IDS techniques for IoT networks at the edge, such as inspecting network protocols [28], determining application services [29], and identifying abnormal patterns at the edge [30]. Existing IDSs have led to evolve and improve deep learning, statistical learning, and machine learning systems to classify massive data by analyzing the threats of IoT networks [11,31].

2.3 Related Work

Several IDSs have been proposed in the literature to identify cyber-attacks from network systems. For instance, Sadek et al. [32] proposed a new hybrid IDS approach using an indicator variable-enabled rough set technique for feature reduction and neural networks for classification. The empirical results revealed that the hybrid approach could achieve a 96.7% accuracy and a 3% false alarm rate using the NSL-KDD dataset, with lower computational resources than other compelling IDSs. The authors in [33] suggested a hybrid IDS based on the triangle area based nearest neighbors (TANN). The k-mean algorithm was used to cluster centers of attack classes, and KNN was used for classifying attack events. This experiment showed high accuracy and a low false alarm rate on the KDD-Cup 99 dataset.

Moustafa et al. [5] proposed a new approach called (ODM-ADS) that detects attacks, where a new profile was designed to model normal events and detect attacks differently based on an outlier function. This approach would be deployed at IoT and cloud and fog computing, and it accomplished high performances compared with other techniques using the NSL-KDD dataset and UNSW-NB15 datasets. Essam et al. [34] proposed a hybrid algorithm based on correlation feature selection and information gain to reduce the number of features. This research applied to the NSL-KDD dataset; the reduced dataset was validated by a naive Bayes classifier using the adaptive boosting technique. A study by Alom et al. [35] used DBN to perform an intrusion detection system for detecting unknown attacks. Karimi et al. [36] developed a feature selection technique using information gain and symmetric uncertainty model to select the relevant features and naïve Bayes for classifying attacks. The outputs showed that the proposed techniques performed more than machine learning-based IDSs.

Tang et al. [37] developed an intrusion detection model using a deep forward network that contains three hidden layers. The model used the best six features selected from the NSL-KDD dataset. Ling et al. [38] applied a convolution neural network technique for IDS that detect attacks. Niyaz et al. [39] used the auto-encoder to get feature representation then classify the data

using the soft-max regression using the NSL-dataset. Hodo et al. [40] proposed a new approach of an artificial neural network to detect DoS and DDoS attacks with obtaining good accuracy in IoT systems. Chen et al. [41] also tried to detect DDoS for IoT networks. Haddadi et al. [42] used two hidden layers of the neural network using the DARPA1999 data to overcome the problem of overfitting and detect suspicious events. Amma et al. [43] proposed a new in-depth radial approach to optimize the depth of the neural network parameters applied to different datasets to detect DoS attacks.

Recently, Moustafa et al. [1] reviewed existing IDSs and their methods and problems in network and edge systems. The authors demonstrated that the main challenge of IDSs is that existing IDS approaches cannot discover new families from large-scale and heterogeneous data sources collected from IoT networks. It was recommended that deep learning techniques improve the performance of reliable intrusion detection systems for obtaining high detection accuracy and low false alarm rates [1,16]. Therefore, this study's primary goal is to discover new attack families from heterogeneous data sources collected from the edge of a network. Deep learning is used in this work as it has the ability of the feature extracting, analyzing in deep, and detecting suspicious vectors.

3 Proposed CNN-Enabled Intrusion Detection System

This section discusses the proposed Intrusion Detection System (IDS) that discovers cyber-attacks from the edge of a network. The proposed system provides the ability to deal with the essential features of network flows. The proposed system includes three main components: data preprocessing, feature selection, and decision engine, as depicted in Fig. 1. In data preprocessing, network data are filtered and processed by removing redundant values, converting data into a numeric format, and normalizing data to improve feature selection and decision engine stages. In feature selection, the information gain method is applied to select the essential features and enhance the accurate detection of the decision engine technique. In the decision engine, a few shot deep learning-based Convolution Neural Network (CNN) techniques are employed to classify anomalous behaviors. The three components of the proposed IDS are explained below.

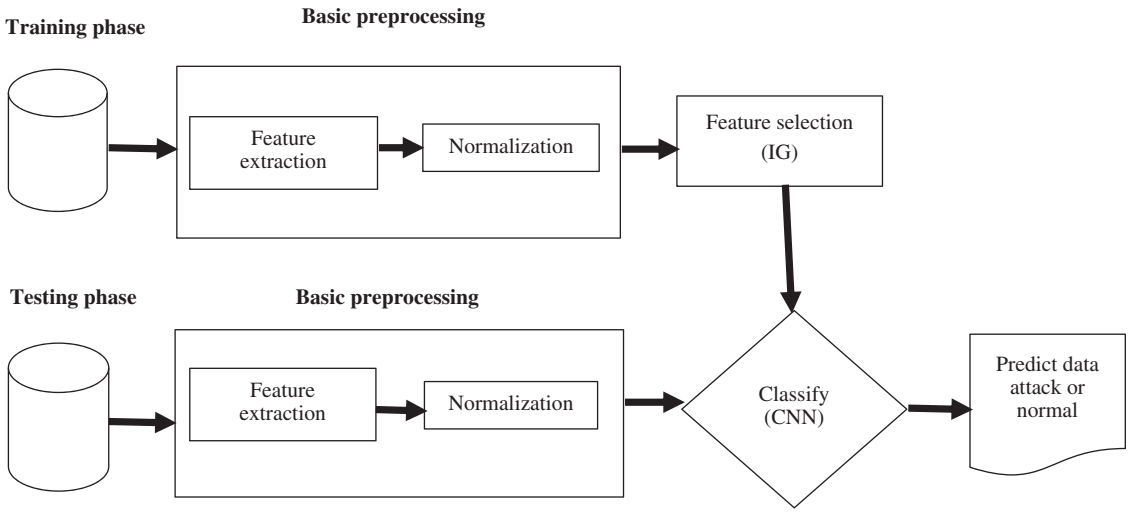

Figure 1: Architecture of the proposed IDS system

3.1 Data Preprocessing Phase

In the data preprocessing phase, network data are filtered by converting non-numerical features to numerical values because the convolution neural network handles numbers. This conversion happens by converting categorical values in the datasets into numeric ones, such as protocol values in the dataset are converted into numerical values, for example, (TCP = 1, UDP = 2, ICMP = 3). Redundant values in the datasets are also excluded to enhance the detection accuracy of Deep Learning. To overcome the imbalance in the datasets, the train and test data are divided into 20% testing data and 80% training data. The values of the feature datasets, such as UNSW-NB 15 and BoT-IoT datasets, are entirely different because the data have nominal, float, and timestamp values. Therefore, data features are normalized into a range of values, such as [0,1], to improve the decision engine's performance.

3.2 Few Shot Learning Method for Intrusion Detection

Few-Shot Learning (FSL) can release new tasks that have only a few samples with supervised information. In other words, FSL is a new machine learning that is ready to learn from a limited number of examples with supervised information [44,45]. FSL can help in the robotics field [46], which generates robots or machines that act like humans. Many fields need to use FSL, and the most important one is drug discovery, which finds out the properties of new molecules to generate a new drug [9] that will be useful for diseases. FSL is now considered a hot topic because it is based on a small number of samples, so many machine learning approaches have been proposed, such as embedding learning [47,48], meta-learning [49], and generative modeling [44,50].

3.2.1 Feature Selection-Based Information Gain (IG)

Information Gain (IG) is known as mutual information that indicates a training set of features vectors is most useful for discriminating between the classes to be learned and tries to find a subset of the original variable, which is calculated as Eq. (1). It is one of three feature selection strategies: filter, wrapper, and embedded approaches [16]. It is used to improve the accuracy of the system or time for mining. The different researchers applied data preprocessing techniques, such as data cleaning, data integration, and dimensionality reduction based on feature reduction and feature selection. The entropy determines the value of the information and relation between each feature, estimated as Eq. (2). Feature selection is the way of searching for a solution to make a network more secure through reducing false alarm and time costs of IDSs during monitoring malicious activities on a network.

The objective of feature selection is to minimize the attribute. It led to making probability close to possible original distribution to all attributes. This process is done without more selection techniques employed to select relevant and information features or to select features that are useful to build a good predictor. Information gain is based on Shannon's mathematical theory and communication and depends on entropy, which is a measure of unpredictability of information, and ranks the features that affect the data classification and pi is the probability of feature in the given set of features as shown in Eq. (3).

$$\mathrm{I.G} = \mathrm{entropy(feature)} - [\mathrm{average\ \ entropy\ \ (other\ \ features)}] \tag{1}$$

where

$$\mathrm{Entropy} = \sum\nolimits_i \mathrm{p_i log_2 p_i} \tag{2}$$

$$\mathrm{Pi} = (\#\ \mathit{classes}_i / \mathit{entity\ population}) \tag{3}$$

According to Maher and Ulrich (2012), IG handles only discrete values; therefore, it is essential to transfer continuous values into discrete values. Given the two random variables X and Y, I (X, Y) is the information gain of X concerning the class attribute Y. When Y and are discrete variable that takes values in $\{y_i,\ldots, y_t\}$ and $\{x_i,\ldots, x_t\}$. With probability distribution function P(x); then the entropy of X is given by Eq. (4) or average information is expected value of I(x) over an instance of X by Eq. (5). Information I from the message X. Hence the IG for feature F on the dataset D in Eq. (6)

$$\mathrm{H(x)} = -\sum_{\mathrm{i=1}}^{\mathrm{t}} (\mathrm{p(X=xi)}\ \ \mathrm{log2(p(X=xi))} \tag{4}$$

$$\mathrm{H(x)} = E_x(I(x)) \tag{5}$$

$$IG(D,F) = H(D) - \sum_{\mathrm{attr=value}} \left[\frac{|D_{\mathrm{attr}}|}{|D|} * H(D_{\mathrm{attr}}) \right] \tag{6}$$

where value (F) is the set of all possible F values, D_{attr} is the subset of D that has a value attr. H(D) = entropy of the class attribute.

Based on the information gain method, we select the most critical ten features from the network datasets to improve the decision engine technology's performance that can discover cyber-attacks.

3.2.2 Convolution Neural Network (CNN) as Decision Engine

CNN is used as a decision engine of IDS that classifies legitimate and anomalous activities at the network's edge. CNN may be a later type of neural network that works on to memorize and reach appropriate features for speaking to the input information. There are two contrasts with MLPs, which are weight sharing and pooling. CNN has numerous layers, and each layer comprises numerous convolution bits that are utilized to form distinctive outlines. Each locale of the neuron of a feature outline is connected to the following layer. All the spatial areas of the input share the bit for producing the included outline. One or different completely connected layers are utilized for the classification [13] after a few convolution and pooling layers. Since the utilization of shared weights in a Convolution Neural Network, the demonstration learns the same design is happening at distinctive positions of inputs without inquiring about memorizing isolated detectors for each position. For that, the architecture can control the interpretation of inputs [51].

The pooling layers minimize the computational obstacle since it diminishes the number of connections between convolutional layers. Be that as it may, pooling layers expanding the properties of interpretation and upgrading the open field of convolution layers. The activation function is used to solve non-linearity for convolution neural networks that help multi-layer detect nonlinear features. There are three types of activation function sigmoid, tanh and ReLU. One or numerous completely connected layers can be included after the stream of the network. To measure the blunders within the preparing portion, loss work can be utilized to check the mistakes [52]. The CNN is adapted using the parameters listed in Tab. 1 to establish a decision engine technique that can classify legitimate and attack events of datasets collected from the edge of networks.

Table 1: Adapted hyperparameters of CNN used as a decision engine

Layer (Type)	Output shape	Number of parameters
conv1d_1 (Conv1D)	(None, 10, 32)	128
leaky_re_lu_1 (LeakyReLU)	(None, 10, 32)	0
max_pooling1d_1 (MaxPooling1)	(None, 5, 32)	0
conv1d_2 (Conv1D)	(None, 5, 64)	6208
leaky_re_lu_2 (LeakyReLU)	(None, 5, 64)	0
max_pooling1d_2 (MaxPooling1)	(None, 3, 64)	0
conv1d_3 (Conv1D)	(None, 3, 128)	24704
leaky_re_lu_3 (LeakyReLU)	(None, 3, 128)	0
max_pooling1d_3 (MaxPooling1)	(None, 2, 128)	0
flatten_1 (Flatten)	(None, 256)	0
dense_1 (Dense)	(None, 128)	32896
leaky_re_lu_4 (LeakyReLU)	(None, 128)	0
dense_2 (Dense)	(None, 2)	258

4 Experimental Results

4.1 Experimental Design

We used Google open-source data flow engine TensorFlow using the Python Keras package, which is named Google Colab [53], to implement the proposed IDS. Keras was used as the front-end API as it is the foremost critical library in an in-depth convolutional network study. It incorporates a model reinforcement to utilize it effectively and rapidly that runs utilizing CPU and GPU.

4.2 Datasets Used

To validate the proposed system for different types of attacks and different network infrastructure and characteristics, testing and evaluation was carried out on two different network datasets of UNSW-NB15 [14] and BoT-IoT [15,54]. First, the UNSW-NB15 [14] is a new data set published in 2015 from The UNSW Canberra Cyber to evaluate intrusion detection purposes. The UNSW-NB15 is divided into a training set and testing set containing 175,341 records and testing 82,332 records. The UNSW-NB15 used the IXIA Perfect Storm tool to establish mixed regular and modern attacks of network traffic. The UNSW-NB15 includes nine attack families, as demonstrated in Tab. 2.

Second, the Bot-IoT dataset was designed from a real network environment and was built in the cyber range lab of UNSW Canberra to be used for creating. There are combinations between normal and malicious traffic in the environment. The source files of the datasets are given with different formats that contain CSV files, PCAP files, and argue files. The files will be clustered based on the attack category and subcategory to get better support in the labeling process. The PCAP files are 69.3 GB, with more than 72.000.000 records. The size of the extracted traffic is 16.7 GB. MySQL queries are used in the botnet dataset for extracting 5% of the original dataset to ease the usage of the dataset. The extracted 5% consists of 4 files 1.07 GB in size, and 3 million records. The attack types of the Bot-IoT dataset are described in Tab. 3.

Table 2: Attack types of UNSW-NB15 dataset

Attack types	Description
Fuzzers	It is an attack; the attacker tries to find out vulnerabilities of the application and network. Supply it with the vast inputting of indistinctive data to make it shatter.
Analysis	This attack is related to a web application. An attacker sneaks the web application from a port scan, web scripts and spam of emails.
Backdoor	It is a technique of passing hidden standard authentication; make the authorization of remote access to an end device, the definition of the access to plain text, as it wants to be unobserved.
DoS	It is an intrusion which disrupts the computer resources via memory to cause excessive business, to prevent authorized requests from accessing a device.
Exploit	It is an asset of orders which pick advantage of vulnerability, unsuspected manner on network or host.
Generic	This attack uses a hash function to make collision without esteem to the arrangement of the block–chipper. This attack makes against block-cipher.
Reconnaissance	It is the same meaning of probe; the attacker begins to collect the information about the network of the computer to shirk the security.
Shellcode	It is malware in which the attacker sneaks a small part of code starting from a shell to control the machine.
Worm	It is an attack in which the attacker replicates itself to propagate on computers and use network computers to spread, based on the security washout of the accessing computer that uses it.

Table 3: Attack types of Bot-IoT dataset

Attack types	Description
Port scanning	are malicious activities that gather information about victims through scanning active ports in remote systems that could be used for exploiting them.
OS fingerprinting	are suspicious activities that try to collect information about target systems by scanning active operating systems through a network.
DoS attacks	are malicious activities that try to corrupt a service, thus making it unavailable to normal users.
DDoS attacks	are intrusive events that corrupt systems using multiple DoS attacks.
Data theft	is a group of attacks where an adversary seeks to compromise the security of a machine to obtain sensitive data.
Keylogging	are malicious programs developed to monitor and record all keystrokes of victims secretly.

4.3 Feature Selection Using Information Gain

The ten crucial features are selected using the Information Gain technique from the UNSW-NB15 and BoT-IoT datasets, as listed in Tabs. 4 and 5. These features are used as the input of

applying CNN as a decision engine to classify normal and attack activities. They significantly impact the performance of the decision engine by improving the detection accuracy and processing time.

Table 4: Best ten features from the UNSW-NB15 dataset

Feature name	Feature description
dmean	Mean of the flow packet size transmitted by the destination
ackdat	TCP connection setup time, the time between the SYN_ACK and the ACK packets.
ct_dst_ltm	Number of records of the same destination IP address in 100 records according to the record last time
ct_src_dport_ltm	Number of records of the same source IP address and the destination port number in 100 records according to the record last time
ct_srv_dst	Number of connections that contain the same service and destination address in 100 connections according to the last time
dbytes	Destination to source transaction bytes
dloss	Destination packets retransmitted or dropped
dintpkt	Destination inter-packet arrival time (mSec)
Dtcpb	Destination TCP base sequence number
Dpkts	Destination to source packet count

Table 5: Best ten features from the Bot-IoT dataset

Feature name	Feature description
Daddr	Destination IP address
N_IN_Conn_P_DstIP	Number of inbound connections per destination IP
Proto	Textual representation of transaction protocols presents in network flow
Max	Maximum duration of aggregated records
State number	Numerical representation of feature state
Mean	Average duration of aggregated records
Min	Minimum duration of aggregated records
Stddev	Standard deviation of aggregated records
Sport	Source port number
Seq	Argus sequence number

4.4 Results of CNN Compared with Other IDSs

The proposed CNN-IDS model was trained using the two datasets of UNSW-NB15 and Bot-IoT. This phase of training to guarantee that parameters dependable for affecting in the testing phase. The evaluation of the CNN intrusion detection system was processed on the ten selected features of datasets listed in Tabs. 4 and 5. Using the UNSW-NB15 dataset, the overall Detection

Rate (DR) and False Positive Rate (FPR) of the CNN-IDS are represented in Fig. 2. In this figure, the Receiver Operating Characteristics (ROC) curves which show the relation between the detection rates and false rates, are depicted. The outcomes demonstrated the proposed system could detect different attack types in an average of 91% on the UNSW-NB15 dataset. The results of CNN-IDS system is compared with four existing intrusion detection techniques, that are named the Triangle Area Nearest Neighbors (TANN) [33], Euclidean Distance Map (EDM) [55] and Multivariate Correlation Analysis (MCA) [56], Outlier Dirichlet Mixture (ODM) [5]. As shown in the figure, the system outperforms these techniques in terms of detection rate with about 2% and a false positive rate with roundly 1%–2%.

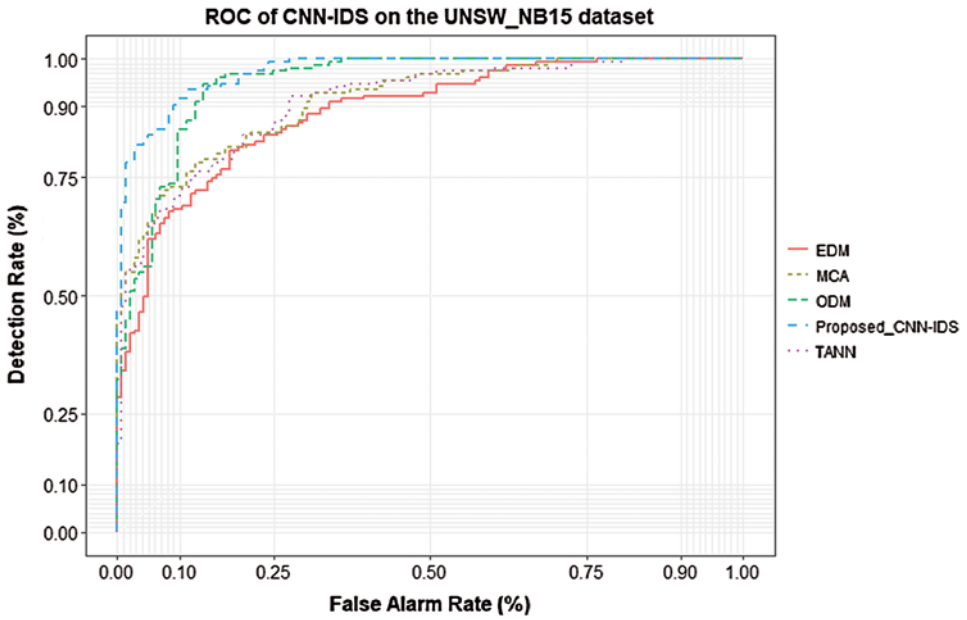

Figure 2: ROC curve of CNN-IDS compared with other techniques on the UNSW-NB15 dataset

The proposed CNN-IDS system also can correctly classify and discover various attack types using the BoT-IoT dataset, as presented in Fig. 3. The proposed system can detect all the attack types in around a 99.9% detection rate and a 0.01% false-positive rate on the BoT-IoT dataset. The CNN-IDS system is also compared with the four techniques used in the UNSW-NB15 dataset. The outputs illustrated that the proposed system would detect attack types better than other models with about a 3% detection rate and around a 3%–4% false-positive rate. When comparing the results on both datasets, it is obvious that the proposed CNN-IDS achieves better performance with about 8% detection rate using the BoT-IoT dataset that is higher than the UNSW-NB15. This is because the BoT-IoT has new attack types with high variations between the normal and attack classes, enabling the CNN-IDS system to train the normal and attack data better than the UNSW-NB15 dataset.

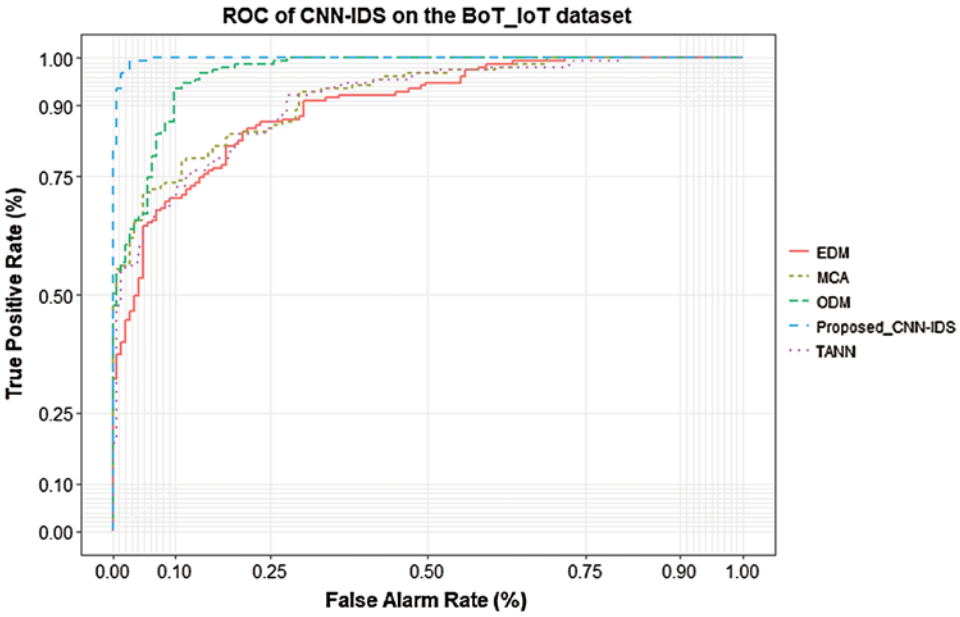

Figure 3: ROC curve of CNN-IDS compared with other techniques on the BoT-IoT dataset

To sum up, the proposed CNN-IDS system achieves higher detection accuracy than the other four IDS mechanisms because of its potential design using the Information gain and CNN models. The Information Gain assisted in selecting the most important features in both datasets, while the CNN architecture [57] was designed to have multi-dense layers that can identify small variations between the normal and abnormal events from the datasets. Therefore, the proposed system can be used as a proper IDS solution that identifies and alerts attack activities at the edge of networks.

5 Conclusion

This paper has presented a new IDS, so-called CNN-IDS, based on a few shots learning. The proposed CNN-IDS has been developed to discover new attack events from the edge of a network. The proposed system includes two models of feature selection and decision engine. The feature selection model was developed by the Information Gain method to select essential features from network data, while the decision engine was developed using a one-dimensional Convolutional Neural Network (CNN) algorithm to discover attack events. The proposed system was trained and tested using two datasets of the UNSW-NB15 and Bot-IoT. The results showed that the proposed system outperforms several peer intrusion detection systems. This demonstrates the capability of applying the proposed system at real IoT networks and safeguards them against new cyber threats. This work will be extended by developing new federated IDS that can concurrently discover attacks from IoT services and their network traffic.

Funding Statement: This work has been supported by the Australian Research Data Common (ARDC), project code–RG192500.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Moustafa, J. Hu and J. Slay, "A holistic review of network anomaly detection systems: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 128, pp. 33–55, 2019.

[2] M. Elrawy and A. Awad, "Intrusion detection systems for IoT-based smart environments: A survey," *Journal of Cloud Computing*, vol. 7, pp. 1–20, 2018. https://doi.org/10.1186/s13677-018-0123-6.

[3] R. Sadek, "An agile internet of things (IoT) based software defined network (SDN) architecture," *Egyptian Computer Science Journal*, vol. 42, no. 9, pp. 13–29, 2018.

[4] R. Sadek, "Hybrid energy aware clustered protocol for IoT heterogeneous network," *Future Computing and Informatics Journal*, vol. 3, no. 2, pp. 166–177, 2018.

[5] N. Moustafa, K. Choo, I. Radwan and S. Camtepe, "Outlier dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 1975–1987, 2019. https://doi.org/10.1109/TIFS.2018.2890808.

[6] S. Anwar, J. Zain, M. Zolkipli, S. Khan, Z. Inayat *et al.*, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, pp. 1–24, 2017.

[7] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire and P. R. M. Inácio, "Security challenges of the internet of things," in *Beyond the Internet of Things*, Cham: Springer, pp. 53–82, 2017. https://doi.org/10.1007/978-3-319-50758-3_3.

[8] W. Trappe, R. Howard and R. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security*, vol. 13, no. 1, pp. 14–21, 2015.

[9] A. Hassan and A. Awad, "Transition in the era of the internet of things: Social implications and privacy challenges," *IEEE Access*, vol. 6, pp. 36428–36440, 2018.

[10] J. King and A. Awad, "A distributed security mechanism for resource-constrained IoT devices," *Informatica (Slovenia)*, vol. 40, no. 1, pp. 133–143, 2016.

[11] S. Chawla, "Deep learning-based intrusion detection system for internet of things," Master of Science in Cyber Security Engineering, University of Washington, Dissertation, 2017.

[12] Y. Wang, Q. Yao, J. Kwok and L. Ni, "Generalizing from a few examples: A survey on Few-shot learning," *Association for Computing Machinery*, vol. 1, no. 1, pp. 1–34, 2020.

[13] R. Vinayakumar, K. Soman and P. Poornachandran, "Applying convolutional neural networks for network intrusion detection," in *Int. Conf. on Advances in Computing, Communications and Informatics*, Udupi, India, pp. 1222–1228, 2017.

[14] N. Moustafa and J. Slay, "UNSW-Nb15: A comprehensive data set for network intrusion detection systems (UNSW-nB15 network data set)," in *Military Communications and Information Systems Conf.*, Canberra, ACT, Australia, IEEE, pp. 1–7, 2015.

[15] N. Koroniotis, N. Moustafa and E. Sitnikova, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[16] M. AL-Hawawreh, N. Moustafa and E. Sitnikova, "Identification of malicious activities in the industrial internet of things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[17] S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh *et al.*, "Intelligent feature selection and classification techniques for intrusion detection in networks: A survey," *Journal of Wireless Communications and Networking (EURASIP)*, vol. 1, pp. 1–16, 2013.

[18] W. Bul'ajoul, A. James and M. Pannu, "Improving network intrusion detection system performance through quality of service configuration and parallel technology," *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 981–999, 2015.

[19] S. Gautam and H. Om, "Computational neural network regression model for host-based intrusion detection system," *Perspectives in Science*, vol. 8, pp. 93–95, 2016.

[20] E. Bertino and N. Islam, "Botnets and internet of things security," *Cybertrust*, vol. 50, no. 2, pp. 76–79, 2017.

[21] A. Abduvaliyev, A. Pathan, J. Zhou, R. Roman, C. Wong *et al.*, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communcations Surveys Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[22] B. Caswell and J. Hewlett, "Snort the open source network intrusion detection system," 2016. [Online]. Available: https://www.snort.org.

[23] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguous and discontinuous system call patterns," *IEEE Transactions Computer*, vol. 63, no. 4, pp. 807–819, 2014.

[24] N. Moustafa, B. Turnbull and K. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815–4830, 2018.

[25] M. Eskandari and Z. Janjua, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE*, vol. 7, no. 8, pp. 1–1, 2020. https://doi.org/10.1109/JIOT.2020.2970501.

[26] T. Marsden, N. Moustafa, E. Sitnikova and G. Creech, "Probability risk identification-based intrusion detection system for scada systems," in *Int. Conf. on Mobile Networks and Management*, Melbourne, Australia, vol. 235, pp. 353–363, 2017.

[27] M. Conti, A. Dehghantanha, K. Franke and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Science Direct*, vol. 78, pp. 544–546, 2018.

[28] E. Adi, Z. Baig and P. Hingston, "Stealthy denial of service (DOS) attack modelling and detection for http/2 services," *Journal of Network and Computer Applications*, vol. 91, pp. 1–13, 2017.

[29] T. Qiu, N. Chen, K. Li, M. Atiquzzaman and W. Zhao, "How can heterogeneous internet of things build our future: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2011–2027, 2018.

[30] D. Shreenivas, S. Raza and T. Voigt, "Intrusion detection in the rpl-connected 6lowpan networks," in *Proc. of the 3rd ACM Int. Workshop on IoT Privacy, Trust, and Security*, Abu Dhabi, United Arab Emirates, ACM, pp. 31–38, 2017.

[31] S. Duquea and M. Omar, "Using data mining algorithms for developing a model for intrusion detection system (IDS)," *Procedia Computer Science*, vol. 61, pp. 46–51, 2015.

[32] R. Sadek, M. Soliman and H. Elsayed, "Effective anomaly intrusion detection system based on neural network with indicator variable and rough set reduction," *International Journal of Computer Science Issues*, vol. 10, no. 2, pp. 227–233, 2013.

[33] C.-F. Tsai and C.-Y. Lin, "A triangle area based nearest neighbors' approach to intrusion detection," *Pattern Recognition*, vol. 43, no. 1, pp. 222–229, 2010.

[34] Y. Essam, E. El salamouny and G. Eltaweel, "Improving the performance of multi-class intrusion detection systems using feature reduction," *International Journal of Computer Science*, vol. 12, no. 3, pp. 255–262, 2015.

[35] M. Alom and V. Bontupalli, "Intrusion detection using deep belief network and extreme learning machine," *International Journal of Monitoring and Surveillance Technologies Research*, vol. 3, no. 2, pp. 35–56, 2015.

[36] Z. Karimi, M. Mansour and A. Harounabadi, "Feature ranking in intrusion detection dataset using combination of filtering methods," *International Journal of Computer*, vol. 78, no. 4, pp. 21–27, 2013.

[37] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep recurrent neural network for intrusion detection in sdn-based networks," in *2018 4th IEEE Conf. on Network Softwarization and Workshops*, Montreal, QC, Canada, IEEE, pp. 202–206, 2018. https://doi.org/10.1109/NETSOFT.2018.8460090.

[38] S. Ling and L. Mohammadpour, "A convolutional neural network for network intrusion detection system," *Aesthetics Practitioners Advisory Network*, vol. 46, pp. 1–6, 2018.

[39] A. Javaid, Q. Niyaz, W. Sun and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. of the 9th EAI Int. Conf. on Bio-Inspired Information and Communications Technologies (formerly BIONETICS)*, New York, United States, pp. 21–26, 2016. https://doi.org/10.4108/eai.3-12-2015.2262516.

[40] E. Hodo, X. Bellekens, A. Hamilton, P. Louis Dubouilh, E. Iorkyase *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *Int. Symp. on IEEE Networks, Computers and Communications*, Yasmine Hammamet, Tunisia, pp. 1–6, 2016.

[41] R. Chen, M. Liu and C. Chen, "An artificial immune-based distributed intrusion detection model for the internet of things," *Advanced Materials Research*, vol. 366, pp. 165–168, 2012.

[42] F. Haddadi and S. Khanchi, "Intrusion detection and attack classification using feed-forward neural network," in *Second Int. Conf. on Computer and Network Technology*, Bangkok, Thailand, pp. 262–266, 2015. https://doi.org/10.1109/ICCNT.2010.28.

[43] N. Amma and S. Selvakumar, "Deep radial intelligence with cumulative incarnation approach for detecting denial of service attacks," *Neurocomputing*, vol. 340, pp. 294–308, 2019.

[44] L. Fei, R. Fergus and P. Perona, "One-shot learning of object categories," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 4, pp. 594–611, 2006.

[45] M. Fink, "Object classification from a single example utilizing class relevance metrics," in *Advances in Neural Information Processing Systems*, New York, USA: Curran Associates, Inc., pp. 449–456, 2005.

[46] J. Craig, *Introduction to Robotics: Mechanics and Control*, Noida, Uttar Pradesh: Pearson Education India, 2009.

[47] L. Bertinetto, J. Henriques, J. Valmadre, P. Torr and A. Vedaldi, "Learning feed-forward one-shot learners," in *NIPS'16: Proc. of the 30th Int. Conf. on Neural Information Processing Systems*, Barcelona, Spain, pp. 523–531, 2016.

[48] O. Vinyals, C. Blundell, T. Lillicrap, D. Wierstra *et al.*, "Matching networks for one shot learning," in *Advances in Neural Information Processing Systems*, Barcelona, Spain, pp. 5530–5538, 2016.

[49] C. Finn, P. Abbeel and S. Levine, "Model-agnostic meta-learning for fast adaptation of deep networks," in *Int. Conf. on Machine Learning*, Sydney, Australia, pp. 1156–1154, 2017.

[50] H. Edwards and A. Storkey, "Towards a neural statistician," in *Int. Conf. on Learning Representations*, Palais des Congrès Neptune, Toulon, France, pp. 1–13, 2017.

[51] A. Kapoor and H. Fan, "Intelligent detection using convolutional neural network (ID-cNN)," *Earth and Environmental Science*, vol. 234, pp. 1–10, 2019.

[52] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, vol. 9, no. 20, pp. 1–28, 2019.

[53] Google Colab, https://colab.research.google.com/notebooks/intro.ipynb#recent=true, February 2020.

[54] N. Moustafa and J. slay, "UNSW-Nb15 dataset," 2015. [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/.

[55] Z. Tan, A. Jamdagni, X. He, P. Nanda and R. Liu, "Denial-of-service attack detection based on multivariate correlation analysis," in *Int. Conf. Neural Information Processing System*, Shanghai, China, pp. 756–765, 2011.

[56] Z. Tan, A. Jamdagni, X. He, P. Nanda and R. Liu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Transactions Parallel Distribution System*, vol. 25, no. 2, pp. 447–456, 2014.

[57] M. Gamal, H. Abbas and R. Sadek, "Hybrid approach for improving intrusion detection based on deep learning and machine learning techniques," *Joint European-US Workshop on Applications of Invariance in Computer Vision*, Cairo, Egypt, vol. 1153, pp. 225–236, 2020.